Bijlage: advies FG

Voorlegger RvB: Afspraken over het gebruik van ChatGPT e.d. binnen UWV

5 september 2023

Het is goed dat er aandacht is voor dit onderwerp en de bijbehorende kansen en risico's.

Mijn advies is om generatieve AI-toepassingen, zoals ChatGPT, **niet** als 'niet-risicomijdend' in te zetten en in elk geval het gebruik van vrij toegankelijke AI toepassingen als ChatGPT **niet** toe te staan. De privacyrisico's van het gebruik van dergelijke toepassingen zijn aanzienlijk en de verwerking van persoonsgegevens is niet transparant. UWV zal een standpunt moeten innemen óf, onder welke voorwaarden en binnen welke kaders zij generatieve AI toepassingen wil inzetten. Ik adviseer daarbij om daar waar gesproken wordt over Chat GPT dit te vervangen door Generatieve AI (GEN-AI). Daaronder vallen bijvoorbeeld Large Language Models, maar ook andere toepassingen. De privacyrisico's spelen namelijk ook bij dergelijke soortgelijke toepassingen.

Generatieve AI-toepassingen moeten m.i. uitsluitend worden ingezet in een gecontroleerde omgeving met bijhorende duidelijke kaders. Het op te stellen kader zal moeten aansluiten bij de bestaande afspraken binnen de organisatie zoals de governance, UWV Beleidskaders Privacy, de Gedragscode en het Kompas Data Ethiek. Ik vraag me dan ook af of het nodig is een apart ethisch kader op te stellen voor het gebruik van GEN-AI. Uiteraard kan wel overwogen worden het huidige kompas aan te vullen met kaders m.b.t. dit onderwerp.

Daarnaast moet beoordeeld worden of een GEB voor de toepassing van GEN-AI-tools noodzakelijk is. Meer informatie over het GEB-proces is te vinden op DWU. Voor GEB's die betrekking hebben op verwerkingen die gebruik van algoritmen voor bijvoorbeeld het opstellen van klantprofielen, risicomodellen of voor geautomatiseerde besluitvorming is als hulpmiddel een speciale bijlage ('Bijlagen bij GEB-rapport – Risico-inventarisatie & algoritmen') opgesteld. Deze bijlage bevat een toelichting op de informatie die in een dergelijke GEB moet worden opgenomen, en kan worden gebruikt om een goede afweging te maken m.b.t. de inzet van GEN-AI voor een bepaalde verwerking. Daarbij wordt bijvoorbeeld gekeken naar doelbinding, proportionaliteit, noodzaak en transparantie.

Advies is om op korte termijn helder te communiceren naar alle UWV-medewerkers wat het standpunt van UWV is m.b.t. de inzet van GEN-AI-toepassingen. Gelijktijdig kan dan in rustiger tempo gewerkt worden aan een zorgvuldige inrichting van een proeftuin waarbij goed gekeken wordt naar de privacyrisico's en maatregelen en kunnen de risico's op het juiste niveau vooraf worden geaccepteerd.

Gezien de hoge privacyrisico's adviseer ik te overwegen om de toegang tot ChatGPT en soortgelijke toepassingen vanuit het UWV-netwerk in de tussentijd (tijdelijk) te blokkeren.